
USER'S MANUAL

SymPA v 0.1

University of Málaga, Spain

September, 2007

Technical report ITI 07-2.

Authors: Almudena Díaz Zayas
 Pedro Merino Gómez
 Laura Panizo Jaime
 Álvaro M. Recio Pérez
 Francisco Javier Rivas Tocado

PLEASE READ CAREFULLY THE FOLLOWING TERMS OF USE. BY USING THE TOOL YOU AGREE TO BE BOUND BY THESE TERMS. IF YOU DO NOT AGREE TO BE BOUND BY THE TERMS OF USE, DO NOT USE THE TOOL.

Material and tools may be downloaded from our website for personal and non-commercial use only, but it is forbidden to alter or remove any trademark, copyright or other such notification from the material.

Neither the authors nor any other physical or legal entity who may have participated in the development of this tool may be held liable for damage to property or loss of profit that users might incur as a result of its use.

Revision Sheet

Release No.	Date	Revision Description
Rev. 0	11/09/07	First Release

This tool has been developed with the effort and the support of Almudena Díaz Zayas, Pedro Merino Gómez, Laura Panizo Jaime, Alvaro Recio Pérez and F^o Javier Rivas Tocado.

USER'S MANUAL

TABLE OF CONTENTS

	<u>Page #</u>
1.0 GENERAL INFORMATION.....	1-1
1.1 System Overview.....	1-1
1.2 Points of Contact.....	1-2
1.3 Organization of the Manual.....	1-2
2.0 SYSTEM SUMMARY.....	2-1
2.1 Installation Guide	2-1
2.1.1 Installing SymPA in Series 60 Smartphone by Application Manager of PC Suite	2-2
2.1.2 Installing SymPA via Infrared or Bluetooth	2-4
2.1.3 Installing SymPA in the terminal.....	2-4
3.0 GETTING STARTED.....	3-1
3.1 System Menu	3-1
3.1.1 Capture.....	3-2
3.1.2 PDP Context Info.....	3-4
3.2.2.1 Network Interface Information	3-5
3.1.2.2 Packet-switched Connection Context Information	3-6
3.1.2.3 Negotiated values for GPRS/UMTS Rel99 and UMTS Rel4 QoS profile	3-6
3.2.3 Ping.....	3-7
3.2.4 Mobile to Mobile File Transfer	3-8
3.2.5 Cell Info	3-9
3.2.6 Log file	3-11
4.0 Use cases.....	4-2
4.1 Live Capture	4-2
4.2 Info Maps	4-2
4.3 Experimental Results	4-3

1.0 GENERAL INFORMATION

1.0 GENERAL INFORMATION

1.1 System Overview

SymPA is a protocol analyzer for mobile phones that allows all the incoming TCP/IP traffic to be captured without interfering with the normal performance of the terminal. The main design goals for this tool have been the following:

- To capture all incoming IP packets, while avoiding information overload.
- To perform efficient resource management, according to constraints on power processing and battery life of mobile devices.
- To include basic functions for network management such as ping, PDP (Packet Data Protocol) context info etc.
- To provide interfaces for processing captured information and exporting it to other environments.
- Analysis of security problems in mobile devices.
- Debugging of network protocols over cellular networks.
- Debugging of new protocols for new mobile services.
- Detection of bugs in network protocol implementations for mobile devices.
- Detection of irregular behavior of traditional protocols in mobile environments.

1.2 Points of Contact

www.lcc.uma.es/~pedro/mobile

1.3 Organization of the Manual

This document provides a user's guide for SymPA. It describes SymPA installation, basic usage and configuration.

2.0 SYSTEM SUMMARY

2.0 SYSTEM SUMMARY

SymPA mobile application enables traffic analysis and monitoring of mobile devices in real operating conditions. With this tool it is possible to sniff all of the IP traffic that other applications running on a mobile phone receive from GPRS/UMTS connections. This makes SymPA particularly suitable for studying the end-to-end performance of IP based protocols and for mobile peer-to-peer scenarios. In addition, the application provides useful information related to radio parameters and the state of the mobile device, which can be used to detect the cause of transmission problems.

From our point of view it is crucial to provide developers with tools similar to those used for local area networks such as ping, tracer, netstat, sniffers,...

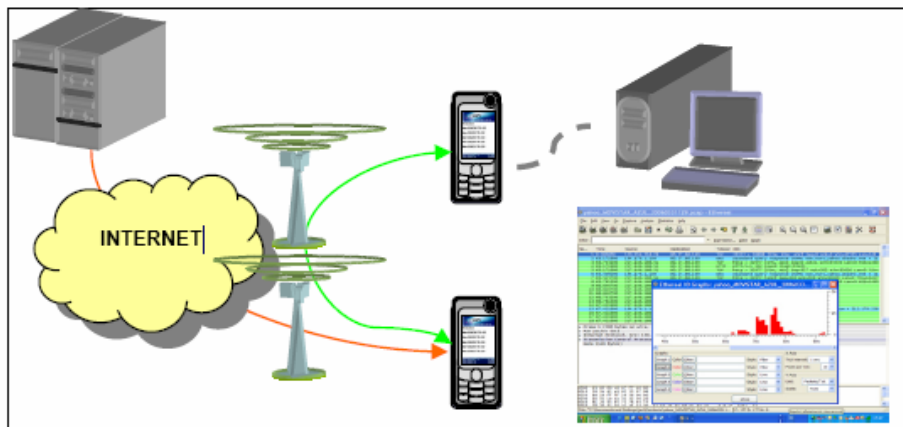


Figure 1. SymPA working diagram

2.1 Installation Guide

This release has been tested on Serie 60 devices with different operating systems. In Symbian 7.0s and Symbian 8.0a all functionalities work, whereas in Symbian 6.0 PDP Context Info functionality is limited to a few parameters only.

The Symbian 9.0 version is also available but it is not public due to security restrictions.

2.1.1 Installing SymPA on a Series 60 Smartphone using the Application Manager of the PC Suite

1. In the PC Suite Menu click on the "Install applications" option.

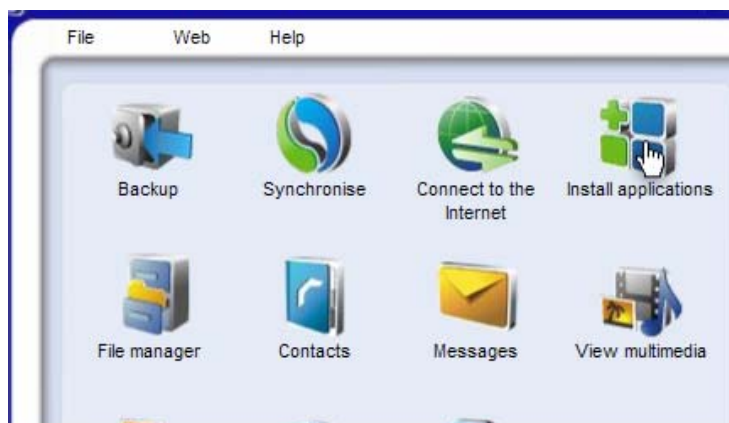


Figure 2. PC Suite Installation. Step 1

2. In the Applications installer on the left side, you can browse from "my computer" and select the .SIS file you wish to install.

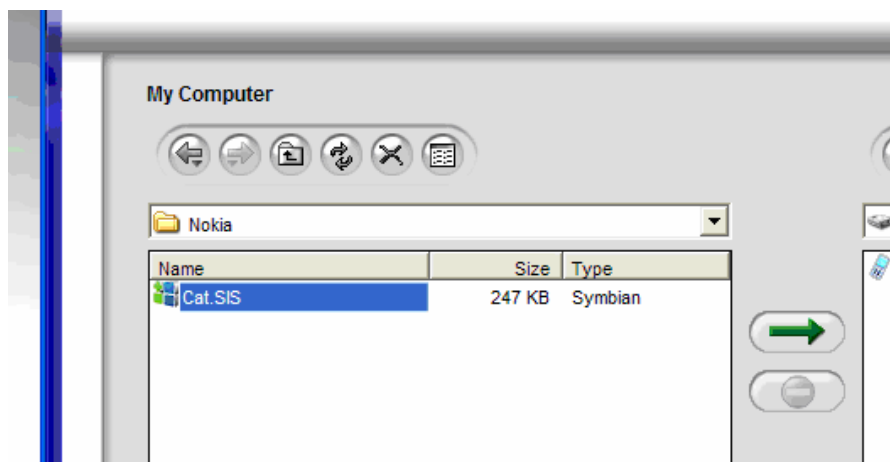


Figure 3. PC Suite Installation. Step 2

3. Next click on the arrow pointing to the right

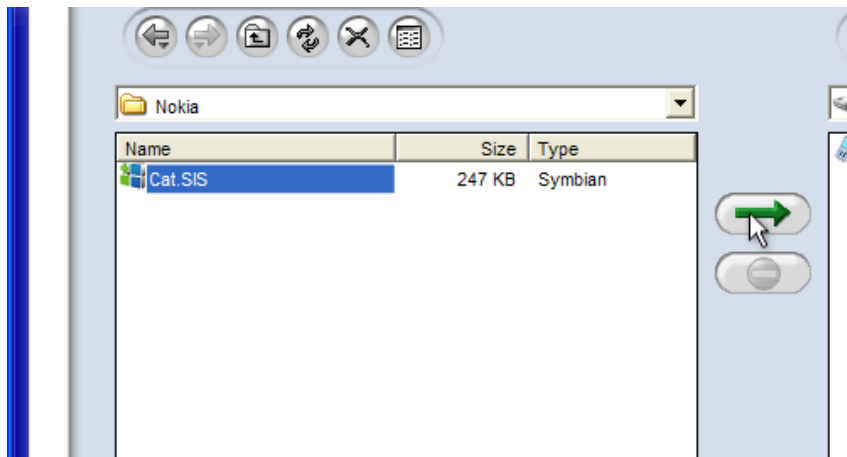


Figure 4. PC Suite Installation. Step 3

4. The application will be transferred to the mobile device and the installation will begin on the mobile phone.



Figure 5. PC Suite Installation. Step 4

2.1.2 Installing SymPA via Infrared or Bluetooth

The installation file can be transferred to the mobile device via Infrared or Bluetooth. The .SIS file will be stored in the "Inbox" as a message and when the message is opened the installation starts.

2.1.3 Installing SymPA in the terminal

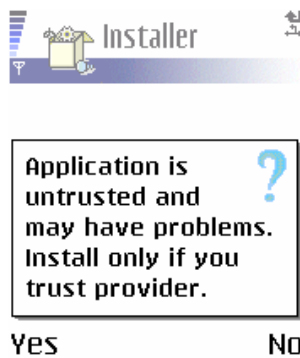


Figure 6. Terminal installation. Step 1



Figure 7. Terminal installation. Step 2

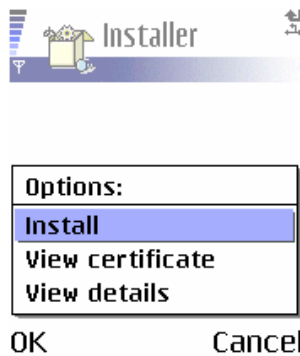


Figure 8. Terminal installation. Step 3

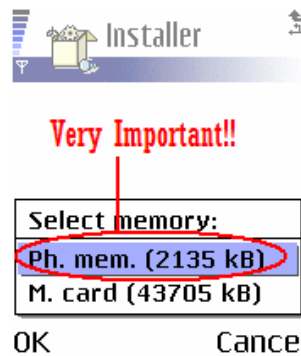


Figure 9. Terminal installation. Step 4

It is very important to install the application in the phone memory!!!

Eliminado: ¶

3.0 GETTING STARTED

3.0 GETTING STARTED

In this section menus available for using the application are described.

3.1 System Menu

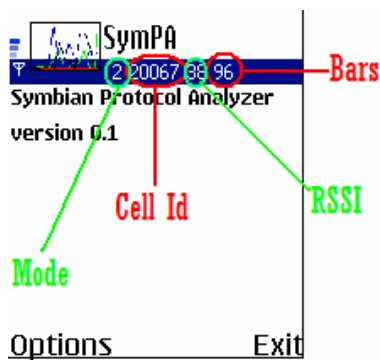


Figure 10.1 Initial view

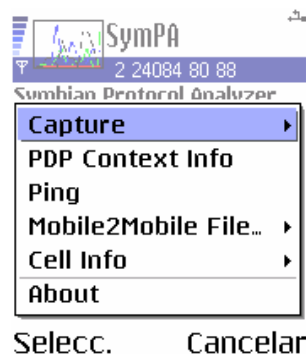


Figure 11. Initial Menu

In the initial view of the application, at the top, cell information is shown. This information is updated every second. The information available is the following:

- **Mode**
Network Modes
 - 0 Unknown
 - 1 Unregistered
 - 2 Gsm
 - 3 Amps
 - 4 Cdma95
 - 5 Cdma2000
 - 6 Wcdma
- **Cell Id**
Cell Global Identifier
- **RSSI (- dBm)**
Radio Signal Strength Indicator. Signal strength
- **Bars**
Signal bars phone displays

3.1.1 Capture

When SymPA is in capture mode, all IP packets reaching the mobile devices from GPRS/UMTS connections are saved in a file in raw format. SymPA runs in the background without interfering with the performance of active applications. In parallel, network parameters can be observed periodically. When the capturing session finishes, capture is transformed to text2pcap input format. The lipcap format conversion tool is included in the free distribution of the Wireshark analyzer. The files can be transferred to a computer via USB, infrared or Bluetooth, depending on the terminal availability of these technologies. Lipcap files can be analyzed directly with Wireshark, taking advantage of the great variety of filtering options, statistical analysis and graph generation features of this application.

The capture functionality is launched from main menu "Capture/Start Capture" when the application capturing a "C" is shown in the navigation pane? (figure 13).



Figure 12. Capture Menu

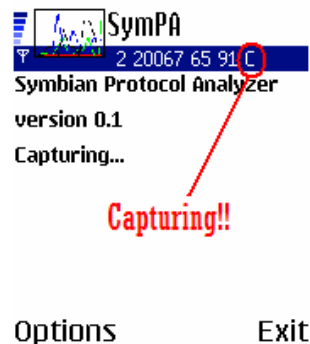


Figure 13. Capturing

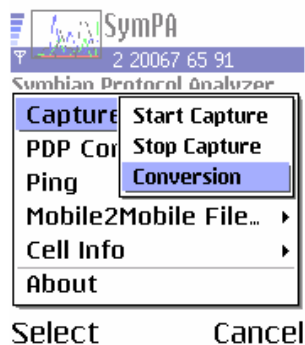


Figure 14. Conversion Menu

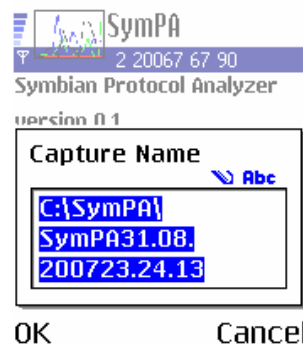


Figure 15. File we want to convert

All the traffic captured is stored in a file located in the C:\SymPA directory. The name of the file contains the date and time when the capture was initiated (figure 16). When it finishes, this file can be converted to the input format of text2cap tools using the conversion option shown in figure 14.

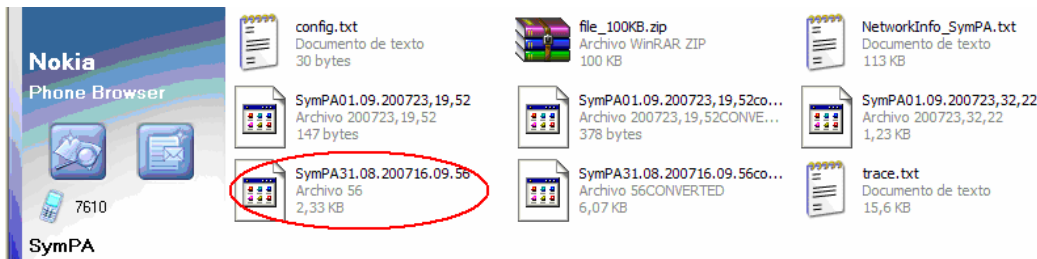


Figure 16. Capture File

The resulting file (figure 17) is transferred to the PC using a PC Suite or other technology such as Infrared or Bluetooth. Once the file is in the PC we can convert it to libpcap format so we can visualize it using a traditional Protocol Network Analyzer, such as Wireshark.

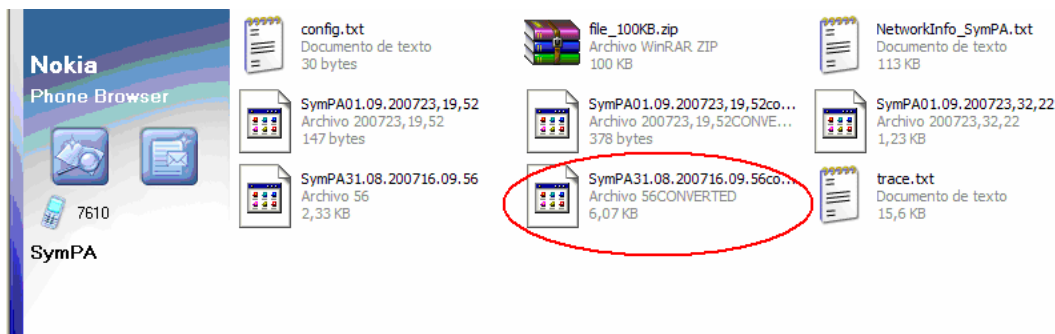


Figure 17. Converted File

```

05/05/200611:31:45,3437 000000 45 00 00 40 4d 88 40 00 2f 06 18 7c 96 d6 d6 1c d5 04 a3 bc 77 24 92 21 f8 df d4 8a 2f
05/05/200611:31:46,0625 000000 45 00 00 34 4d 89 40 00 2f 06 18 87 96 d6 d6 1c d5 04 a3 bc 77 24 92 21 f8 df d4 8b 2f
05/05/200611:31:46,3906 000000 45 00 00 de 4d 8a 40 00 2f 06 17 dc 96 d6 d6 1c d5 04 a3 bc 77 24 92 21 f8 df d4 8b 2f
05/05/200611:31:47,3906 000000 45 00 04 01 4d 8b 40 00 2f 06 14 b8 96 d6 d6 1c d5 04 a3 bc 77 24 92 21 f8 df d5 35 2f
05/05/200611:31:48,2812 000000 45 00 01 bc 4d 8c 40 00 2f 06 16 fc 96 d6 d6 1c d5 04 a3 bc 77 24 92 21 f8 df d9 02 2f
05/05/200611:31:49,3437 000000 45 00 01 bc 4d 8d 40 00 2f 06 16 fb 96 d6 d6 1c d5 04 a3 bc 77 24 92 21 f8 df da 8a 2f
05/05/200611:31:53,8437 000000 45 00 01 63 4d 94 40 00 2f 06 17 4d 96 d6 d6 1c d5 04 a3 bc 77 24 92 21 f8 df dc 12 2f
05/05/200611:31:54,4218 000000 45 00 01 2a 6d 43 00 00 6f 11 f7 3b 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 16 02 e1 8f
05/05/200611:31:54,4218 000000 45 00 00 70 6d 44 00 00 6f 11 f7 f4 96 d6 d6 1c d5 04 a3 bc 1b 3b 1b 83 00 5c 5f a0 8f
05/05/200611:31:54,4531 000000 45 00 01 b9 6d 45 00 00 6f 11 f6 aa 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 01 a5 34 75 8f
05/05/200611:31:54,5781 000000 45 00 00 70 6d 46 00 00 6f 11 f7 f2 96 d6 d6 1c d5 04 a3 bc 1b 3b 1b 73 00 5c bc 84 8f
05/05/200611:31:54,6875 000000 45 00 01 28 6d 48 00 00 6f 11 f7 38 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 14 3d 76 8f
05/05/200611:31:54,8281 000000 45 00 01 25 6d 49 00 00 6f 11 f7 3a 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 11 17 fb 8f
05/05/200611:31:55,0625 000000 45 00 01 32 6d 4a 00 00 6f 11 f7 2c 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 1e e9 57 8f
05/05/200611:31:55,6875 000000 45 00 04 c2 6d 4b 00 00 6f 11 f3 9b 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 04 ae db 68 8f
05/05/200611:31:56,2187 000000 45 00 01 29 6d 4f 00 00 6f 11 f7 30 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 15 e1 2d 8f
05/05/200611:31:56,2343 000000 45 00 03 66 6d 4c 00 00 6f 11 f4 f6 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 03 52 eb ae 8f
05/05/200611:31:56,2812 000000 45 00 01 22 6d 4e 00 00 6f 11 f7 36 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 0e bc 29 8f
05/05/200611:31:56,8281 000000 45 00 05 32 6d 4f 00 00 6f 11 f3 25 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 05 1e e9 5e 8f
05/05/200611:31:56,9062 000000 45 00 00 c2 6d 4e 00 00 6f 11 f7 94 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 00 ae ae 73 8f
05/05/200611:31:57,0000 000000 45 00 01 27 6d 43 00 00 6f 11 f7 2e 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 13 15 c0 8f
05/05/200611:31:57,1250 000000 45 00 01 27 6d 44 00 00 6f 11 f7 2d 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 13 3d f5 8f
05/05/200611:31:57,2500 000000 45 00 01 2a 6d 45 00 00 6f 11 f7 29 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 16 dd 70 8f
05/05/200611:31:57,6406 000000 45 00 03 fd 6d 46 00 00 6f 11 f4 55 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 03 e9 8d d3 8f
05/05/200611:31:57,9375 000000 45 00 03 81 6d 47 00 00 6f 11 f4 d0 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 03 6d 81 46 8f
05/05/200611:31:58,3125 000000 45 00 01 6a 6d 48 00 00 6f 11 f6 e6 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 56 d1 a2 8f
05/05/200611:31:58,5000 000000 45 00 01 48 6d 49 00 00 6f 11 f7 07 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 34 20 08 8f
05/05/200611:31:58,7812 000000 45 00 04 75 6d 4a 00 00 6f 11 f3 d9 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 04 61 01 d6 8f
05/05/200611:31:59,1406 000000 45 00 02 db 6d 4b 00 00 6f 11 f5 72 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 02 c7 dc 95 8f
05/05/200611:31:59,2656 000000 45 00 01 2f 6d 4c 00 00 6f 11 f7 1d 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 1b 58 8f
05/05/200611:31:59,3906 000000 45 00 01 29 6d 4d 00 00 6f 11 f7 22 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 15 49 66 8f

```

Figure 18. Converted File Format. Text2cap input

The file shown in figure 18 is the input of the text2cap tool provided with the Wireshark Protocol Analyzer. A .bat file example is available on the web site to use the text2cap utility, but before doing so, users need to check the time format which appears in the timestamps of a capture file as shown in figure 18 circled in red. This is because changes in the timestamp format depend on the internal configuration of the mobile device. The time format must be in 24h clock format and not pm/am format although this issue will be fixed in future releases to make the conversion seamless.

This is an example of using the text2cap utility. The time format appearing in the converted file obtained from the SymPA tool should agree with that used in the call to the text2cap utility.

```
text2pcap.exe -l 12 -t %%d/%%m/%%Y%%H:%%M:%%S, %1 %1.pcap
```

3.1.2 PDP Context Info

This functionality has been tested over GSM and UMTS networks. Information provided can be divided into three categories:

3.2.2.1 Network Interface Information

Nifs Number of packet network interfaces.

Context Name Name of the context defined for the network interface.

Context Type

- 0 Unspecific context type
- 1 Internal created context
- 2 Externally created context

Nif Status Network Interface Status

- 0 Unknown
- 1 Not activated
- 2 Activating
- 3 Active
- 4 Deactivating
- 5 Suspended
- 6 Deleted



Figure 19. Network interface info

Context Number Number of context belonging to the network interface.

PDP Address PDP Address of network interface.

Conn Status Packet data connection status

- 0 Unattached
- 1 Attached to network but the packet data connection is inactive
- 2 Attached to network and the packet data connection is active
- 3 Attached to network but the packet data connection is suspended

3.1.2.2 Packet-switched Connection Context Information

Connection Speed Connection bandwidth in bits per second

Bytes Sent Number of bytes transmitted over the airlink since its activation

Overflow Sent Number of bytes overflow during the transmission

Bytes Received Number of bytes received

Overflow Recv Number of bytes overflow during reception

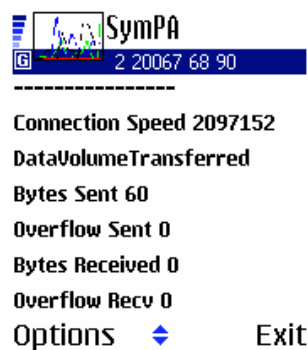


Figure 20. PDP Context Info

3.1.2.3 Negotiated values for GPRS/UMTS Rel99 and UMTS Rel4 QoS profile

BER Negotiated target bit error rate

Deliver Erroneous SDU Negotiated target service data unit error ratio

- 1 Unspecific
- 2 Erroneous SDUs delivered. Error detection not considered
- 4 Erroneous SDUs delivered plus error indication. Error detection used
- 8 Erroneous SDUs discarded. Error detection used.

Deliver Order reqd Negotiated value for sequential SDU delivery

- 1 Unspecific
- 2 Required to be in sequence
- 4 Not Required to be in sequence

Guaranteed Bit Rate Downlink Downlink bitrate in kbps

Guaranteed Bit Rate Uplink Uplink bitrate in kbps

Max Rate downlink Maximum downlink bitrate negotiated in kbps

Max Rate Uplink Maximum uplink bitrate negotiated in kbps

Max SDU size Negotiated maximum SDU size (octets)

SDU error ratio Target SDU Error Ratio

Traffic class Negotiated traffic class

Traffic handling priority Negotiated traffic handling priority

Transfer delay Negotiated transfer delay (milliseconds)

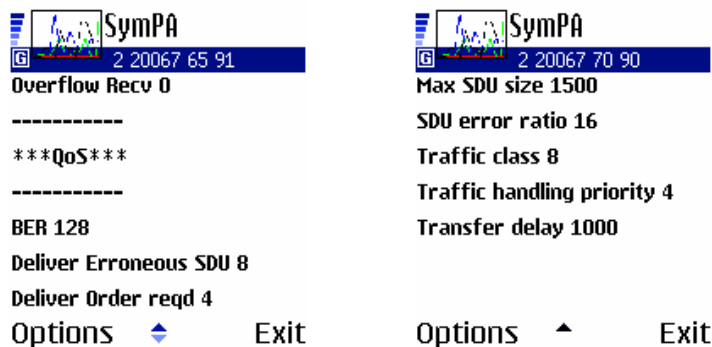


Figure 21. QoS Info

3.2.3 Ping

Traditional ping utility. Time is measured in microseconds.

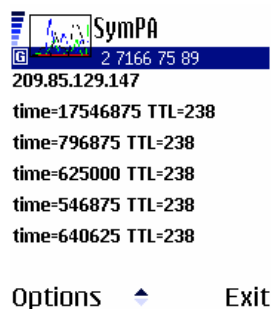


Figure 22. Ping

3.2.4 Mobile to Mobile File Transfer

This utility allows us to transfer a text file between two mobile devices using TCP sockets. The size of the file is fixed to 100kB, in future releases this value will be configurable.

Using this functionality, SymPA enables testing of mobile-to-mobile communications. In this way this tool allows the detection of anomalies and incorrect configurations in TCP implementations used in mobile terminals. These anomalies could appear due to degradation caused by factors which are only present in the mobile environment such as handover. This kind of scenario is therefore very difficult to reproduce. In this use case, it is especially important to use SymPA for real time monitoring.

Capturing the traffic between two mobile devices allows the mobile to mobile connection to be characterized.

3.2.4.1 Starting server side

This functionality is launched through the menu "MobiletoMobil../File Transfer Server/Start" as we can see in figure 23.

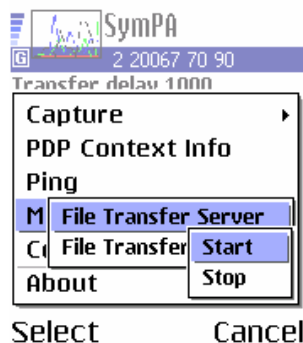


Figure 23. Transfer File. Server Side. Step 1

Once the server opens a new socket and while it is waiting for external connections, the address assigned to the server will appear on the screen (figure 24). This address should be inserted on the client side in order to establish the connection.



Figure 24. Transfer File. Server Side. Step 2

3.2.4.2 Starting client side

On the client side a dialog appears requesting an IP address (Figure 25). We should introduce the address shown on the server side. Then, we press the "OK" button and the connection is initiated.

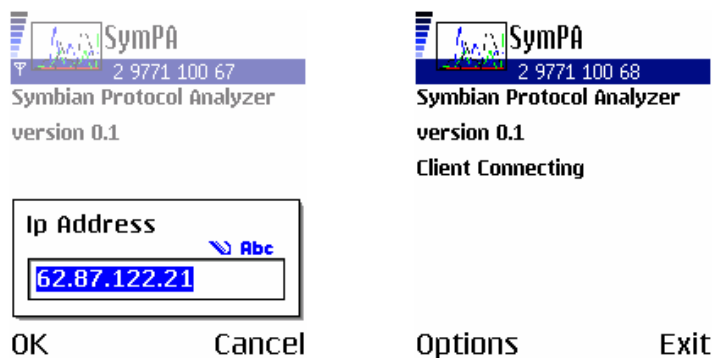


Figure 25. Transfer File. Client Side

3.2.5 Cell Info

The cell info utility offers two different options. The first option "Show Cell Info" shows the information about the cell where the mobile or device is located. The information available is the following:

- CC (Country Code)
- Network Identifier
- Analog SID
- CDMA SID

Tag (Network name)
 Name (Network name)
 Short Name (Network name)
 Cell Identifier
 LAC (Location Area Code)



Figure 26. Network Info

The other function allows us to monitor the cell identifier and network mode. During the monitoring, cell information is stored every second in a file labeled NetworkInfo_SymPa.txt located in the C:\SymPA directory. The file format is shown in figure 29. While this mode is active, an "M" is shown in the navigation pane of the application (Figure 27).

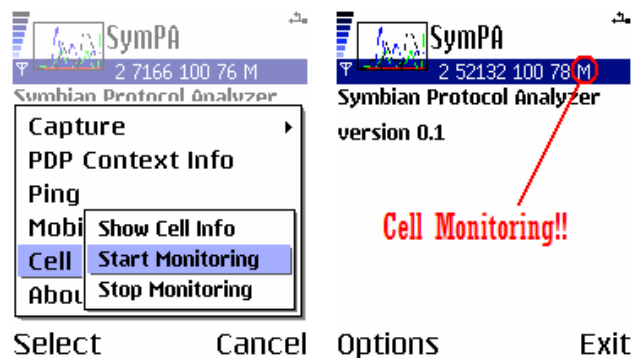


Figure 27. Network Monitoring

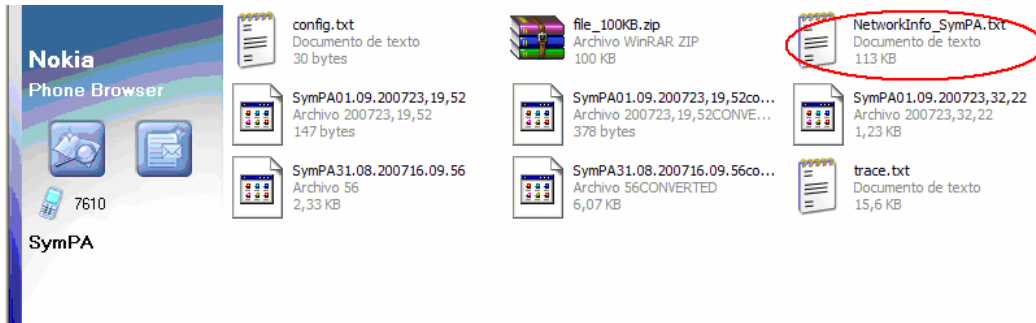


Figure 28. NetworkInfo_SymPA.txt

1	31/08/200710:02:38,4843	2	20621	50	94
2	31/08/200710:02:39,5312	2	20621	50	94
3	31/08/200710:02:40,8750	2	20621	50	94
4	31/08/200710:02:41,8906	2	20621	50	94
5	31/08/200710:02:42,9062	2	20621	50	94
6	31/08/200710:02:43,9218	2	20621	50	94
7	31/08/200710:02:44,9375	2	20621	50	94
8	31/08/200710:02:45,9531	2	20621	50	94
9	31/08/200710:02:46,9687	2	20621	51	93
10	31/08/200710:02:48,0156	2	20621	53	93
11	31/08/200710:02:49,0468	2	20621	55	93
12	31/08/200710:02:50,0781	2	20621	55	93
13	31/08/200710:02:51,1093	2	20621	55	93
14	31/08/200710:02:52,1406	2	20621	54	93
15	31/08/200710:02:53,1718	2	20621	53	93
16	31/08/200710:02:54,2031	2	20621	51	93
17	31/08/200710:02:55,2343	2	20621	50	94
18	31/08/200710:02:56,2656	2	20621	50	94
19	31/08/200710:02:57,3125	2	20621	51	93
20	31/08/200710:02:58,3281	2	20621	55	93
21	31/08/200710:02:59,3593	2	20621	55	93
22	31/08/200710:03:00,3906	2	20621	55	93
23	31/08/200710:03:01,4218	2	20621	55	93
24	31/08/200710:03:02,4687	2	20621	55	93
25	31/08/200710:03:03,4843	2	20621	56	92
26	31/08/200710:03:04,5156	2	20621	60	92
27	31/08/200710:03:05,7187	2	20621	60	92
28	31/08/200710:03:06,7500	2	20621	61	91
29	31/08/200710:03:07,7656	2	20621	60	92
30	31/08/200710:03:08,7812	2	20621	58	92

Date
Network Mode
Bars
RSSI

Figure 29. NetworkInfo_SymPA.txt file format

3.2.6 Log file

A log file is stored in the SymPA directory with all the information shown on the screen of the mobile device. The log file is labeled "trace.txt".

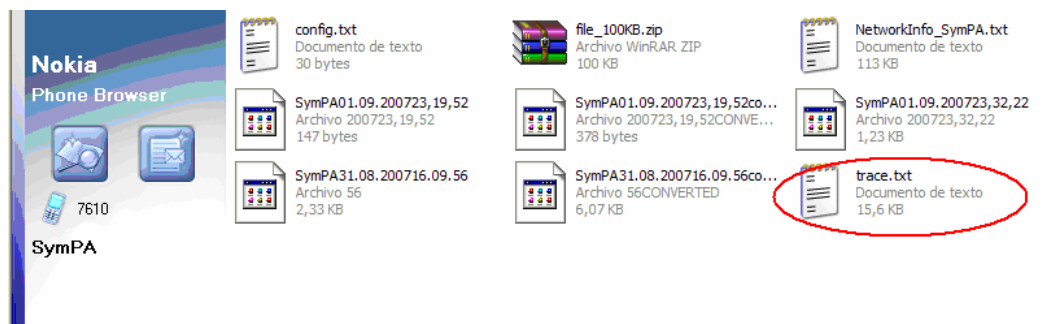


Figure 30. Log File

4.0 USE CASES

4.0 USE CASES

4.1 Live Capture

SymPA allows the capture of traffic received by third applications running on the mobile phone. The normal use of the tool is as follows. First of all, the SymPA tool needs to be launched and the capture mode should be activated. Then the application we want to analyse should be opened. This application will activate a PDP context and SymPA will capture all the traffic received through this context.

As we can see at figure 31 packet captured can be correlated with the rest of the information obtained with SymPA. In figure 31 we can see how a burst of packet losses takes place during a cell change.

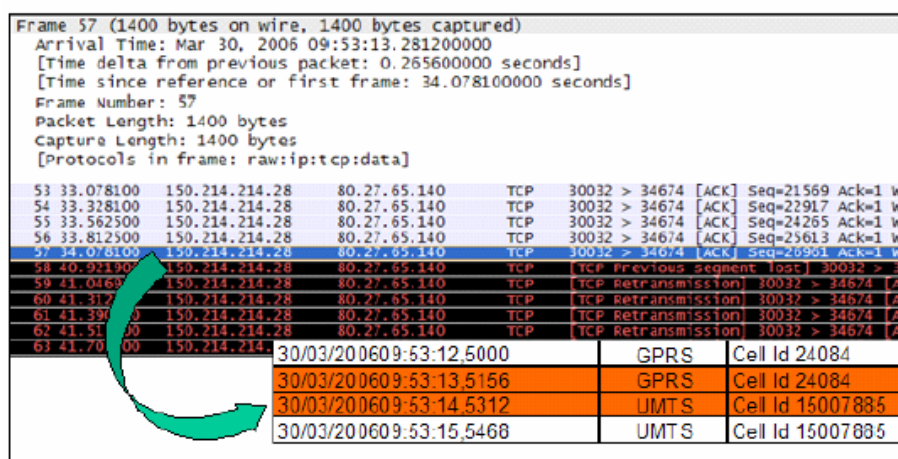


Figure 31. Live capture and cell monitoring

4.2 Info Maps

Cell monitoring and PDP context info functionalities can be used to obtain coverage maps, status maps, and quality of service maps of mobile networks, based on the cell identifier. In future versions of this tool, GPS information will be incorporated, to obtain and store data on the physical location of the cell, in order to establish geographical cell limits.

This point is very interesting in UMTS networks where the geographical area covered by a cell depends on the amount of traffic handled by the cell.

4.3 Experimental Results

This tool has been extensively tested in the performance analysis of video streaming service over cellular networks.

Experimental results can be found in our related works:

- [1] A. Díaz-Zayas, P. Merino, L. Panizo, A.M. Recio, "Evaluating Video Streaming over GPRS/UMTS networks: A Practical Case", in IEEE 65th Vehicular Technology Conference VTC2007-Spring(VTC2007 Spring), 22 - 25 April 2007
- [2] A. Díaz-Zayas, P. Merino, L. Panizo, A.M. Recio, ""Experimental analysis of peer-to-peer streaming in cellular networks", in IEEE 21st International Conference on Advanced Information Networking and Applications (AINA-07), May 21-23 2007
- [3] A. D. Joseph, A. Díaz, P. Merino, F. J. Rivas, U. P. Kulkarni, J. V. Vadavi, G. S. Thyagaraju, S. M. Joshi, and A. R. Yardi, "Mobile and Ubiquitous Objects," IEEE Pervasive Computing, vol. 5, iss. 3, pp. 57–59, 2006.
- [4] A. Díaz, P. Merino, and F. J. Rivas, "Performance Monitoring and Analysis of Wireless Communication Protocols for Mobile Devices," in Proc. 1st International Conference on Ubiquitous Computing: Applications, Technology and Social Issues (ICUC 2006), 2006, pp. 103–108.